BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 31-406

1 APRIL 2000

Security

APPLYING NORTH ATLANTIC TREATY ORGANIZATION (NATO) PROTECTION STANDARDS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at: http://afpubs.hq.af.mil.

OPR: HQ USAF/XOFI (Mr Steven E. Harris)

Certified by: HQ USAF/XOF
(Brig General Richard A. Coleman)

Supersedes AFR 205-43, 6 October 1989)

Distribution: F/Pages: 36

This instruction contains Air Force (AF) unique guidance needed to implement AF Policy Directive (AFPD) 31-4, *Information Security* and supplement United States Security Authority for NATO Affairs (USSAN) Instruction 1-69, *United States Implementation of NATO Security Procedures*, 1982 and DoD Directive 5100.55, *United States Security Authority for North Atlantic Treaty Organization Affairs*, 21 April 1982. All these references together describe how to protect and handle NATO classified information and information releasable to NATO organizations. For user convenience, specific policy references are listed at the end of each paragraph where applicable. Maintain and dispose of all records created as a result of processes prescribed in this instruction in accordance with AFMAN 37-139, *Records Disposition Schedule*. HQ USAF/XOF is delegated approval authority for revisions to this AFI.

SUMMARY OF CHANGES

This is the initial publication of AF Instruction (AFI) 31-406, substantially revising AF Regulation (AFR) 205-43, *Safeguarding NATO Classified Information*. It does not include USSAN 1-69 requirements.

Chapter 1

POLICY AND PROGRAM MANAGEMENT

1.1. Policy. It is Air Force policy to identify, derivatively classify, downgrade, declassify, mark, protect, and destroy classified NATO information and material in its possession as required by NATO policies. This general policy statement also applies to NATO unclassified information consistent with relevant statutes, regulations and directives.

1.2. Applicability. This instruction governs the Air Force NATO Safeguarding Program and takes precedence over all instructions affecting NATO classified material in the possession of Air Force units.

1.3. Program Management. *[Reference USSAN 1-69, ATT 1, paragraph 17]*

1.3.1. The Administrative Assistant to the Secretary of the Air Force (SAF/AA) is the senior Air Force official for the NATO security system within the Air Force, referred to as the Air Force NATO Safeguarding Program.

1.3.2. The Deputy Under Secretary of the Air Force, International Affairs, (SAF/IA) oversees the release of Air Force classified information to foreign governments, persons, and international organizations.

1.3.3. The Chief, Information Security Division (HQ USAF/XOFI) is responsible for formulating policy, resource advocacy, and oversight of the Air Force NATO Safeguarding Program.

1.3.4. Headquarters United States Air Forces in Europe, Security Forces Directorate, Security Programs Division (HQ

USAFE/SFI), is the AF lead office for the NATO Safeguarding Program and as such advises USAF/XOFI on policy, coordinates directives, instructions, and handbooks, and, in conjunction with HQ USAF/XOFI, represents the Air Force at NATO meetings and interagency forums.

1.3.5. Commanders of MAJCOMs, direct reporting units (DRU), field operating agencies (FOA), and installations are responsible for establishing a NATO Safeguarding Program, identifying requirements, and executing their programs to comply with this memo within their activities.

1.3.6. The Information Security Program Manager (ISPM), appointed under AFI 31-401, *Information Security Program Management,* chapter 1, provides policy, guidance, and oversees the activity or installation NATO Safeguarding Program. This responsibility does not include management oversight of the local subregistry.

1.3.7. Commanders of organizations with subregistries are responsible for the overall operation of their subregistries and control points. The unit responsible for Information Management normally manages the local subregistry.

1.3.8. NATO classified material stored inside a Sensitive Compartmented Information Facility (SCIF) is subject to the provisions of this instruction.

1.4. Types of Information.

1.4.1. NATO. The "NATO" marking means the information is the property of NATO requiring the NATO originator's consent for dissemination outside of NATO and is subject to the security protection in this instruction.

1.4.2. ATOMAL. Refers to atomic information provided by the governments of the United States and/or United Kingdom to NATO under the *Agreement Between the Parties to the North Atlantic Treaty Organization for Co-Operation Regarding Atomic Information*.

1.4.3. COMSIC Top Secret (CTS). COSMIC is a NATO marking and designation that is synonymous with Top Secret and is applied exclusively to all copies of Top Secret documents prepared for circulation within NATO. CTS will be applied only to information that the unauthorized disclosure would result in exceptionally grave damage to NATO.

1.4.4. NATO Secret (NS). Applied only to information the unauthorized disclosure of which would result in serious damage to NATO.

1.4.5. NATO Confidential (NC). Applied only to information the unauthorized disclosure of which would result in damage to NATO.

1.4.6. NATO Restricted (NR). The US does not have a security classification equivalent to NATO Restricted. NATO information classified as Restricted shall be safeguarded in a manner that shall prevent disclosure to non-Governmental personnel.

1.4.7. NATO Unclassified (NU). NATO unclassified information may not be released to non-NATO nations, organizations, and individuals without approval of NATO. *[Reference USSAN 1-69, ATT 1, paragraph 4.1]*

1.5. Changes to Policy. Submit recommended changes to this guidance or USSAN 1-69 through ISPM channels to HQ USAF/XOFI. *[Reference USSAN 1-69, ATT 1, paragraph 20]*

1.6. Waivers. Send requests for waivers or exceptions through ISPM channels to HQ USAF/XOFI.

1.7. Inspections.

1.7.1. Include the NATO Safeguarding Program in self-inspections, program reviews, staff assistant visits, and Inspector General inspection/reviews as explained in DoD 5200.1-R, *Information Security Program*, chapter 1, and AFI 31-401, chapter 1.

1.7.1.1. ISPMs will review subregistries when performing program reviews of the servicing unit. ISPM reviews of control points can be used to meet the requirement of paragraph **1.7.2.** below.

1.7.2. Subregistries will inspect their control points at least once every 18 months. As explained in paragraph 1.7.1.1, ISPM reviews may be used to fulfill this requirement. *[Reference USSAN 1-69, ATT 1, paragraph 120]*

1.7.3. The Central United States Registry (CUSR) inspects Air Force CTS, ATOMAL, and NATO Secret subregistries and control points. The CUSR provides written results of the inspection to the activity concerned. Subregistries and control points will forward a copy of CUSR inspection reports to their servicing ISPM. Commanders of subregistries and control points return reports of corrective action directly to the CUSR with an information copy to their servicing ISPM. Recommend local or MAJCOM ISPMs accompany CUSR inspectors during their inspection. *[Reference USSAN 1-69, ATT 1, paragraph 18d, 120, and ATT 2, paragraph 56]*

1.8. Security Education. Include procedures for safeguarding NATO classified information with the required training contained in DoD 5200.1-R, chapter 9, and AFI 31-401, chapter 8.

1.8.1. Foreign Contact/Travel Briefing. For training requirements or briefings pertaining to counter intelligence activities relating to foreign travel or foreign attendance, contact the servicing Air Force Office of Special Investigations (AFOSI) Detachment. *[Reference USSAN 1-69, ATT 1, paragraph 36 & 37]*

1.9. Release of US Classified or Sensitive Unclassified Information to NATO. Do not release US classified information or sensitive unclassified information to NATO without approval from the supporting foreign disclosure office. See AFI 16-201, *Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations*. *[Reference USSAN 1-69, ATT 1, paragraph 3a]*

Chapter 2

CLASSIFICATION MANAGEMENT

2.1. General. Air Force original classification authorities (OCAs) do not originally classify NATO information, but rather U.S. information under the guidelines set forth in DoD 5200.1-R, Chapter 2 and AFI 31-401, Chapter 2.

2.1.1. The principle of classification, marking, downgrading, etc., as outlined in DoD 5200.1-R and AFI 31-401, apply to NATO classified material. *[Reference USSAN 1-69, ATT 1, paragraphs 68 - 74]*

2.1.2. For AF officials that hold both AF positions and NATO positions, DoD 5200.1-R and AFI 31-401 pertain to information classified for exclusive US use and applicable NATO security regulations pertain to information classified for exclusive NATO use. These officials derive NATO classification authority through HQ SHAPE as a result of their position in NATO and not the Department of Defense.

2.2. Derivative Classification. Responsibility for derivative application of NATO classification marking rests with the individuals who include, paraphrase, restate, or generate in new form, information already classified by NATO authorities, or apply classification markings based on guidance from a NATO original classification authority (OCA). Persons who apply derivative classification markings must: *[Reference USSAN 1-69, ATT 1, paragraph 93 and 94]*

2.2.1. Carry forward the NATO classification marking.

2.2.2. Carry forward the assigned date or event of declassification and any other additional markings.

2.3. Challenges to Classification. Challenge the classification of information when a substantial reason to believe the information is classified improperly or unnecessarily exists. *[Reference USSAN 1-69, ATT 1, paragraph 74]*

2.3.1. Send challenges to NATO classified information through ISPM channels to HQ USAF/XOFI. HQ USAF/XOFI will forward challenges to the CUSR for appropriate action.

2.4. Downgrade or Declassification. Air Force personnel may not downgrade or declassify NATO information without the specific consent of the NATO originator. This also applies to extracted NATO classified information in US documents. *[Reference USSAN 1-69, ATT 1, paragraph 76]*

2.5. Reviewing CTS Documents. Annual inventory and "clean out day" under DoD 5200.1-R and AFI 31-401 satisfies this requirement. *[Reference USSAN 1-69, ATT 1, paragraph 77 and 112]*

2.6. Reviewing NATO Secret/Confidential Documents. Annual "clean out day" under DoD 5200.1-R and AFI 31-401 satisfies this requirement. *[Reference USSAN 1-69, ATT 1, paragraph 77.2 and 112]*

Chapter 3

MARKING

3.1. General. Classified material containing the words "COSMIC" or "NATO" before the classification marking indicates the material belongs to NATO. This includes material received from NATO in which the US has original classification authority. *[Reference USSAN 1-69, ATT 1, paragraph 2, 3, and 27]*

3.2. Documents Released into NATO. Before an activity releases a classified or sensitive unclassified document to NATO, the last US activity having custody of the material must apply NATO security markings. Additionally, markings identified in AFI 16-201, chapter 3, will be applied, if applicable. Copies of these documents that stay in US channels are marked as US documents and controlled according to DoD 5200.1-R and AFI 31-401. Mark the file copies with the appropriate statement reflecting releasability, see paragraph **1.9.** of this instruction and AFI 16-201. *[Reference USSAN 1-69, ATT 1, paragraph 78a]*

3.2.1. Reference Numbers. When a US classified document is released into NATO as CTS, NS, or ATOMAL, the servicing subregistry or control point officer assigns a sequential reference number to the document. For electronic messages, include the reference number before downgrading or declassification instruction at the end of the message text. Do not place numbers on copies kept in US channels, treat these as US documents of equivalent classification. Develop reference numbers by using the organizations address symbol, classification abbreviation, a sequential document number, and calendar year (for example: 786CS/NS/01/99). *[Reference USSAN 1-69, ATT 1, paragraph 81 and ATT 2, paragraph 38(e)]*

3.2.2. Copy Numbers. Place a copy number on the outside cover or first page for each Top Secret or Secret document released to NATO. These copy numbers deal with the total number of copies released to NATO (for example, two copies of the same document are released - Copy 1 of 2 or Copy 2 of 2). *[Reference USSAN 1-69, ATT 1, paragraph 81 and 89(a)]*

3.2.3. Page Numbers. Each page of a classified document released to NATO carries a page number. Do not consider pages without printed text as a page. *[Reference USSAN 1-69, ATT 1, paragraph 85]*

3.2.4. Restricted Data and Formerly Restricted Data. Restricted Data and Formerly Restricted Data released into NATO will include the following statement “This document contains United States ATOMIC information (Restricted Data or Formerly Restricted Data) made available pursuant to the NATO Agreement Between the Parties to the North Atlantic Treaty for Co-operation Regarding ATOMIC Information dated June 18, 1964, and will be safeguarded accordingly.” *[Reference USSAN 1-69, ATT 2, paragraph 38(b)(1)]*

3.3. Electronically Transmitted Messages. Address messages intended for NATO to a US element, include the following statement on the first line of text after the US classification "RELEASABLE TO NATO AS NATO (classification)." *[Reference USSAN 1-69, ATT 1, paragraph 78b]*

3.3.1. When necessary to transmit an electronic message directly to a NATO organization, include the following statement on the first line of text after the US classification, “NATO (classification) FOR NATO ADDRESSEES.”

3.3.2. The last line of text of a classified message to NATO shows appropriate reference numbers (Top Secret and Secret), the date or event of downgrading (if applicable), and the date or event of declassification.

3.4. NATO Extracted Information in US Documents. Identify NATO classified information by applying portion marking to the extracted information. Apply US classification or unclassified marking only to portions of the document containing US classified information. Show the overall page marking of documents containing NATO extracts with the US classification designation equivalent. Place the statement "This Document Contains NATO (classification) Information" on the face of the document. *[Reference USSAN 1-69, ATT 1, paragraph 93 and 94]*

3.4.1. Show the source of classification in the "Derived From" line. If the only classified source is NATO information, the "Derived From" line identifies the NATO source as the classification authority. If there is US and NATO classified sources, the "Derived From" line identifies both US and NATO sources or the statement "Multiple Sources". When "Multiple Sources" is used, list each source of classification on the file or record copy of the document.

3.4.2. The “Declassify On” line for AF documents containing NATO classified information will reflect both US and NATO declassification instruction as appropriate. If the NATO information does not contain a declassification instruction, the information falls under one of the exemption rules for automatic declassification under DoD 5200.1-R. The following are exemptions that would be used for NATO information; X5 (reveal foreign government information), 25X6 (reveal information that would seriously and demonstrably impair relations between the US and a foreign government), or 25X9 (Violate a statute, treaty, or international agreement). Other exemptions may also apply. *[Reference USSAN 1-69, ATT 1, paragraph 76, 93 and 94]*

3.4.3. ATOMAL Extracts. When extracting ATOMAL information into US documents: *[Reference USSAN 1-69, ATT 2, paragraph 46]*

3.4.3.1. Portion mark the sections containing the ATOMAL information (i.e. NCA, NSA, CTSA).

3.4.3.2. Mark top and bottom of each page containing an ATOMAL extract with the US equivalent security classification.

3.4.3.3. Mark the cover, or in the absence of a cover, the first page, with the Restricted Data or Formerly Restricted Data warning notice (see DoD 5200.1-R, paragraph 5-208) and the statement "This Document Contains NATO (classification) ATOMAL Information."

3.4.3.4. Include a “Derived From” line but not a declassification date.

3.5. NATO Restricted. When NATO Restricted information is included in an otherwise Unclassified AF document, the following statement shall be affixed to the top and bottom of the cover, or in the absence of a cover, the first page, with “This Document Contains NATO Restricted Information, Safeguarded in Accordance with USSAN Instruction 1-69” and all portions must be marked to identify the information as NATO Restricted (NR), NATO Unclassified (NU), or Unclassified (U). *[Reference USSAN 1-69, ATT 1, paragraph 78c]*

3.5.1. The first line of an otherwise Unclassified AF electronic message containing NATO Restricted extracts will contain “This message contains NATO Restricted information. Safeguard IAW USSAN 1-69.” All portions must be marked to identify the information as NATO Restricted (NR), NATO Unclassified (NU), or Unclassified (U).

3.6. Subjects and Titles. When subjects and titles are classified, include an unclassified short title. When no unclassified title is provided, use the first letter of each word of the classified subject to make an unclassified title. *[Reference USSAN 1-69, ATT 1, paragraph 80]*

Chapter 4

ACCESS

4.1. General. To grant access to NATO classified information (NC, NS, CTS) three elements must be met. *[Reference USSAN 1-69, ATT 1, paragraph 29, 30, and 39]*

4.1.1. Individual must have a current US security clearance equal to or greater than the classification level of the NATO information and meet all requirements for access to US classified information.

4.1.2. Individual must have a need-to-know.

4.1.3. Individual must have been briefed and granted access to the appropriate level in accordance with paragraph **4.9.** of this instruction.

4.2. NATO Access Granting Authority. Commanders and staff agency chiefs designate officials in their headquarters, unit, or activity to grant access to NATO classified information, including ATOMAL information. The access granting authority need not have access to NATO classified information. *[Reference USSAN 1-69, ATT 1, paragraph 30]*

4.2.1. Access granting officials must annually review authorization for access to ATOMAL, see paragraph 4.9.1 of this instruction. *[Reference USSAN 1-69, ATT 2, paragraph 40c]*

4.3. NATO Restricted. Persons requiring access to NATO Restricted documents do not require a security clearance or granted access by a granting authority; however determine the person's need-to-know. Before disclosing NATO Restricted information, inform the person of security protection requirements for safeguarding the information and the consequence of negligent handling. *[Reference USSAN 1-69, ATT 1, paragraph 33]*

4.4. Extracts of NATO Classified Information in US Classified Documents. A US security clearance equal to or greater than the classification level of the information is needing to access this type of document. A NATO access authorization is not required for access to these documents. *[Reference USSAN 1-69, ATT 1, paragraph 93]*

4.5. Access by Non-US Nationals.

4.5.1. Cleared nationals of NATO member nations may have access to NATO classified based upon a written assurance from their appropriate government authority that they have been granted access to NATO classified and a clear need-to-know exists. The final need-to-know determination is always made by the person in possession of the information, although there are times when a government or contract document will include these statements.

4.5.2. Nationals of NATO member nations employed by the AF may be granted access to NATO classified, provided the government of the country which the individual is a citizen has given assurance that the person is authorized and has been granted such access. The home country of the individual grants NATO access. The only time US authorities can grant NATO access to a non-US national is when the individual has an Limited Access Authorization (LAA) as covered in para 4.5.3.

4.5.3. Non-US citizens with an approved LAA, based on a favorable Single Scope Background Investigation (SSBI), who are citizens of NATO member nations may be granted access to NATO

classified, by US authorities, to the level of their LAA, provided a NATO mission essential need-to-know exists.

4.5.4. Non-US citizens who are citizens of non-NATO member nations will not be granted access to NATO classified information.

4.6. Temporary Duty (TDY) Assignments Requiring Access to NATO Classified Information. Parent organizations grant NATO access before a TDY. Include NATO access authorizations in DD Form 1610, **Request and Authorization for TDY Travel of DoD Personnel**. When NATO access requirements arise during a TDY, host commanders assume the responsibility of providing initial and termination briefings.

4.7. Security Clearance Certificates. Access granting authorities must provide security clearance certificates when AF personnel are assigned to a NATO billet, on TDY to a NATO organization, or when requested. See attachment 2 or USSAN 1-69, ATT 3, section VII. A. for a sample certificate. *[Reference USSAN 1-69, ATT 1, paragraph 31]*

4.8. Contractors. The Air Force grants its contractors access to NATO classified information via the DD Form 254, **DoD Contract Security Classification Specification**, block 10g. The contractor is responsible for approving access authorizations for its employees, to include providing initial briefings, rebriefings and debriefings. The Air Force may also conduct these briefings. This should be clearly stated in either the contract Statement of Work, DD Form 254, or Visitor Group Security Agreement. When approved by an Air Force official, contractor access authorizations will be annotated in accordance with paragraphs **4.9.** and 4.10 below.

4.8.1. Visits. For NATO Production and Logistics Organization (NPLO) security clearance and visit procedures see DoD 5220.22-M, *National Industrial Security Operating Manual (NISPOM)*, chapter 10. *[Reference USSAN 1-69, ATT 1, paragraph 40 & 41]*

4.9. Briefings. Personnel must be given a NATO security briefing before access to NATO classified information is granted. A sample NATO briefing is at Attachment 4. NATO granting authorities designate individuals to give NATO briefings. Record briefings on AF Form 2583, **Request for Personnel Security Action**. A sample AF Form 2583 is at Attachment 3. The person receiving the briefing signs in the remarks section of the AF Form 2583. Maintain AF Form 2583 or computer generated roster on file at the unit of assignment until there is no longer a need for the access. Do not transfer it upon permanent change of station (PCS) or permanent change of assignment (PCA). *[Reference USSAN 1-69, ATT 1, paragraph 33c]*

4.9.1. Personnel requiring access to ATOMAL information must receive an ATOMAL briefing prior to access and annually thereafter. A sample ATOMAL briefing is at **Attachment 5**. Record annual rebriefings on the AF Form 2583. *[Reference USSAN 1-69, ATT 2, paragraph 53]*

4.9.2. A computer generated roster may be used in lieu of AF Form 2583 to record NATO access when a large number of personnel need access to NATO classified information (i.e., mobility deployment). As a minimum, the information required in blocks 1, 2, 3, 4, and 9 of the AF Form 2583 must be present on the roster. The briefer and those being briefed must sign the roster acknowledging the briefing.

4.10. Debriefing. Commanders and staff agency chiefs shall appoint officials to debrief personnel who no longer require access to NATO classified information. If an individual's US security clearance eligibility is suspended, removed, or revoked, their access to NATO classified information must be immediately removed and the individual debriefed. Record debriefings on AF Form 2587, **Security Termination Statement**. The AF Form 2587 shall be retained in accordance with AFMAN 37-139, *Records Disposition Schedule*. See attachment 6 for a sample debrief. *[Reference USSAN 1-69, ATT 1, paragraph 33c(3)]*

4.11. Refusal to Sign a Termination Statement. When an individual refuses to execute an AF Form 2587, the supervisor, in the presence of a witness:

4.11.1. Debriefs the individual.

4.11.2. Records the fact that the individual refused to execute the termination statement and was debriefed.

4.11.3. Ensures the individual no longer has access to NATO classified information (i.e. notify co-workers, change combinations to security containers, deny access to secure/sensitive areas, etc.)

4.11.4. Forwards a copy to the servicing ISPM who advises the commander on security information file (SIF) considerations. Refer to AFI 31-501, *Personnel Security Program Management*, chapter 8, for SIF guidance.

4.12. Temporary Access. During wartime, periods of mounting international tension, international contingency operations, or in peacetime during deployments or on-call/exercise duty when emergency measures require, commanders may grant temporary access to CTS information based on a final U.S. Secret clearance and issuance of an interim US Top Secret clearance eligibility, pending completion of an SSBI or the issuance of a final US Top Secret clearance eligibility. The temporary access will be rescinded if unfavorable information is identified in the course of the investigation, see paragraph **4.10.** of this instruction. Refer to AFI 31-501, chapter 3. *[Reference USSAN 1-69, ATT 1, paragraph 45 - 47]*

4.13. NATO Billets. *[Reference USSAN 1-69, ATT 1, paragraph 30 - 32]*

4.13.1. Personnel assigned to a NATO billet, who require access to CTS or COSMIC Top Secret ATOMAL (CTSA), require a SSBI within five years.

4.13.2. Air Force members assigned to a NATO billet who require access to NS, NATO Secret ATOMAL (NSA), NATO Confidential (NC), or NATO Confidential ATOMAL (NCA) require a National Agency Check (NAC) submitted prior to 10 May 1999 or the National Agency Check, Local Agency Checks and Credit Check (NACLC) if submitted 10 May 1999 or after, which are less than five years old.

4.13.3. Civilian employees assigned to a NATO billet who require access to NS, NSA, NC, or NCA require a National Agency Check with Written Inquiries (NACI) if submitted prior to 10 May 1999, and a Access National Agency Check with Written Inquiries and Credit Check (ANACI) for those submitted 10 May 1999 or after. A National Agency Check with Written Inquiries and Credit Checks (NACIC) may also be accepted if it was conducted prior to 3 May 1999 and the individual was granted a security clearance eligibility for a secret security clearance by the 497 IG/INS.

4.13.4. Air Force personnel assigned to NATO billets requiring access to NATO classified information require periodic reinvestigations every five years. Submit periodic reinvestigation requests when

the previous investigation is four years old (48 months) in accordance with AC/35-D/1004, *NATO Security Directive* and AFI 31-501.

Chapter 5

SAFEGUARDING

5.1. Storage. Storage requirements for NATO classified information parallel those for US classified of the same level in accordance with DoD 5200.1-R and AFI 31-401. NATO material can be stored in the same security container as non-NATO information provided the NATO material is physically separated from non-NATO material by at least a file divider. *[Reference USSAN 1-69, ATT 1, paragraph 56a and b]*

5.1.1. NATO classified may be turned over to facilities designated for overnight storage of US information. Facility personnel do not need formal access to NATO classified as long as the NATO documents are placed in a sealed container.

5.2. NATO Restricted. NATO Restricted information may be protected similar to "For Official Use Only" and must be safeguarded in a manner that shall prevent disclosure to non-government personnel. *[Reference USSAN 1-69, ATT 1, paragraph 24]*

5.2.1. NATO Restricted may be stored in filing cabinets, desks or other containers, which are located in rooms where AF or AF contractor internal building security is provided during non-duty hours. Where such internal security is not available, locked buildings or rooms will provide adequate protection as long as AF or AF contractors control the keys/combinations. *[Reference USSAN 1-69, ATT 1, paragraph 56c]*

5.3. Combinations. If combinations to security containers holding NATO classified information are recorded, use Standard Form (SF) 700, **Security Container Information**, Part 2. If the container only stores NATO classified, mark the SF 700, Part 2 with the highest NATO classification therein and control it as a NATO document. If the container contains both US and NATO classified, mark the SF 700, Part 2 with the highest classification contained and the statement "NATO Access Required" and control as a US document. Every individual having access to a security container, in which NATO information classified Confidential and above is stored, must have been granted access to NATO information at the appropriate level. Procedures outlined in paragraph **5.1.1.** are an exception to this policy. *[Reference USSAN 1-69, ATT 1, paragraph 59]*

5.3.1. Combinations to security containers that store any NATO classified will be changed annually. See DoD 5200.1-R, para 6-404b, for additional requirements. *[Reference USSAN 1-69, ATT 1, paragraph 60]*

5.4. Cover Sheets. For NATO classified documents removed from security containers use the following cover sheets: AF Form 144, **Top Secret Access Record and Cover Sheet**, for CTS and CTSA, SF 704, **Secret Cover Sheet,** for NATO Secret and NSA, and SF 705, **Confidential Cover Sheet**, for NATO Confidential and NCA. Write the word "COSMIC", "ATOMAL", or "NATO," as appropriate, on cover sheets. When the originator deems a disclosure record is necessary and places special limitations on NSA and NCA documents, a AF Form 144 will be used. In these cases, cross out the "Top Secret" and replace with appropriate classification (CTSA, NSA, or NCA).

5.5. NATO Extracts. Control and protect US generated documents containing NATO extracts as a US document in accordance with DoD 5200.1-R and AFI 31-401. See paragraph **3.4.** of this instruction for marking requirements.

5.6. Document Control: CTS. Distribute and control CTS documents, including messages, through the AF NATO Registry System. Use AF Top Secret control procedures for accountability for CTS, see AFI 31-401, chapter 5. Keep CTS accountability records separate from US Top Secret records.

5.6.1. Use AF Form 143, **Top Secret Register Page**, or equivalent automated form to maintain records for each document, see AFI 31-401, chapter 5. *[Reference USSAN 1-69, ATT 1, paragraph 127(f)]*

5.6.1.1. Do not prepare accountability records for CTS messages kept in telecommunication facilities on a transitory basis for less than 30 days. Use the telecommunication facility accountability register for this function.

5.6.2. Use AF Form 144 as a disclosure record. All individuals who gain knowledge of the information will sign and print their name. Only one entry per individual is required. *[Reference USSAN 1-69, ATT 1, paragraph 99]*

5.6.3. File inactive AF Forms 143, AF Forms 144, AF Form 310, **Document Receipt and Destruction Certificate**, or other records used reflecting disposition in accordance with AFMAN 37-139. *[Reference USSAN 1-69, ATT 1, paragraph 113(b)]*

5.6.4. Commanders of subregistries and control points appoint one or more properly cleared, disinterested person(s) to conduct an annual inventory of all holdings. Each newly appointed control officer also conducts an inventory before assuming the account. *[Reference USSAN 1-69, ATT 1, paragraph 128]*

5.6.4.1. Subregistry or control point commanders must endorse reports of inventory. Control points send the report to their subregistry. Subregistries send the report to the CUSR. The subregistry will provide a copy of the report to the servicing ISPM. *[Reference USSAN 1-69, ATT 1, paragraph 129]*

5.7. Document Control: ATOMAL. CTSA is controlled in a similar manner to CTS, while NSA and NCA are treated similar to NATO Secret. When the originator deems more control is necessary and places special limitations on NSA and NCA documents, treat and account for those documents as CTSA. Keep ATOMAL accountability records and inventory reports separate from non-ATOMAL records. *[Reference USSAN 1-69, ATT 2, paragraph 42 and 54]*

5.8. Document Control: NATO Secret. Distribute NS documents through the AF NATO Registry System. Action offices will administratively control all NS documents by maintaining an active accountability record on each document. An AF Form 310 or general-purpose work sheet may be used for this purpose. The record must identify the document by showing reference numbers, originator of the document, unclassified subject or short title, date of the document, date received or transferred, and the individual or agency the document was transferred to. The communication center will notify the servicing subregistry or control point of these incoming NS messages as outlined in para **7.4.2.** of this instruction. *[Reference USSAN 1-69, ATT 1, paragraph 100]*

5.8.1. NS exercise messages kept less then 30 days are exempt from active accountability. If NS exercise messages are kept for more than 30 days, the message will be entered into the administrative control system. Non-exercise NS messages received directly from the communications center will be placed into the action office's administrative control system.

5.8.2. File inactive accountability, destruction, and transmission certificates in accordance with AFMAN 37-139. *[Reference USSAN 1-69, ATT 1, paragraph 113(d)]*

5.8.3. Recommend commanders of subregistries and control points appoint one or more properly cleared, disinterested persons to conduct an annual inventory of all NS holdings. Also recommend each newly appointed control officer conduct an inventory before assuming the account.

5.9. Document Control: NATO Confidential and Restricted. NATO Confidential and Restricted information may flow from action office to action office. Recipients do not keep active accountability records for the document unless required by the NATO originator.

5.10. Page Changes. When making page changes to accountable NATO documents use an AF Form 1565, **Entry, Receipt, and Destruction Certificate**, AF Form 143, or AF Form 310 for a receipt, accountability, and destruction certificate for the pages being changed.

5.11. Reproduction. Unit commanders and heads of staff offices designate people to exercise reproduction authority for classified material in their activities. For copiers, facsimile machines, scanners, or any other machines with copying capability determine if they retain any latent images when copying classified, and how to clear them when they do. Any products produced during clearing procedures must be destroyed as NATO classified waste. *[Reference USSAN 1-69, ATT 1, paragraph 63]*

5.11.1. Air Force units, which need additional copies of CTS and CTSA documents, should get them from the NATO originator. *[Reference USSAN 1-69, ATT 1, paragraph 89]*

5.11.1.1. If not practical, the subregistry may authorize reproduction of CTS documents. The subregistry must report the reproduction to the CUSR. The CUSR must approve reproduction of CTSA. Ensure all reproductions are entered into the Air Force accountability and control system, and reporting requirements are met. *[Reference USSAN 1-69, ATT 2, paragraph 43]*

5.11.1.2. All reproductions must be annotated with "Reproduced (date) by authority of (CUSR/ subregistry). Reproduced copy _____ of _____ copies." *[Reference USSAN 1-69, ATT 1, paragraph 89]*

5.11.2. NSA and NCA may be reproduced at the subregistry or control point with subregistry approval. The CUSR must be notified of all ATOMAL reproductions. Users may only reproduce ATOMAL information with approval of the subregistry. *[Reference USSAN 1-69, ATT 2, paragraph 43]*

5.11.3. Holders of NATO Secret and below documents may reproduce the document without specific approval of the NATO originator, subregistry, or control point. Record the number of reproductions on the document from which the reproduction was made and place the statement: "Reproduced Copy _____ of _____ copies." Enter reproductions of NATO Secret documents into the administrative control system. *[Reference USSAN 1-69, ATT 1, paragraph 92]*

5.12. Destruction. NATO classified information will be destroyed in the same manner as US classified material of the same level. Include NATO classified information with the annual "clean out day". Destroy US documents with NATO extracts contained within as a US document. See DoD 5200.1-R, chapter 6, and AFI 31-401, chapter 5 for specific requirements. *[Reference USSAN 1-69, ATT 1, paragraph 112a]*

5.12.1. CTS. Two persons and a destruction record is required for the destruction of CTS. AF Form 143, 310, or 1565 can be used for the destruction certificate. Return CTS material and disclosure records to the subregistry for destruction. Subregistries may authorize control points to destroy CTS material. In this case, forward a copy of the destruction certificate and disclosure record to the subregistry. File destruction certificates in accordance with AFMAN 37-139. *[Reference USSAN 1-69, ATT 1, paragraph 113(a), 113(b), and 113(c)]*

5.12.2. NATO Secret. Two persons and a destruction record is required for the destruction of NATO Secret. AF Form 310, or 1556 can be used for the destruction certificate. File destruction certificates in accordance with AFMAN 37-139. *[Reference USSAN 1-69, ATT 1, paragraph 113(d)]*

5.12.3. ATOMAL. ATOMAL information will be returned to the subregistry or CUSR for destruction. Subregistries may destroy ATOMAL information by the same method as non-ATOMAL NATO information of the same level. *[Reference USSAN 1-69, ATT 2, paragraph 33(f)]*

5.12.4. NATO Confidential and Restricted. Only one person and no destruction certificate is needed unless required by the originator. *[Reference USSAN 1-69, ATT 1, paragraph 113(e)]*

5.13. Emergency Planning. NATO classified information will be included in emergency protection, removal, and destruction as described in DoD 5200.1-R, chapter 6. *[Reference USSAN 1-69, ATT 1, paragraph 114]*

5.14. Classified Meetings and Conferences. See DoD 5200.1-R, chapter 6, AFI 31-401, chapter 5, and AFI 61-205, *Sponsoring or Cosponsoring, Conducting and Presenting DoD Related Scientific Papers at Unclassified and Classified Conferences, Symposia, and Other Similar Meetings*. *[Reference USSAN 1-69, ATT 1, paragraph 131]*

5.15. Information Systems (IS). See AFI 33-202, *Computer Security*. *[Reference USSAN 1-69, ATT 1, paragraph 165]*

5.15.1. Treat extracted NATO information in IS as US classified information of the same level. Mark the material as explained in chapter 3 of this instruction.

5.15.2. Individuals accessing IS's, that are approved to process NATO classified information, must have been formally authorized access in accordance with paragraph **4.9.** of this instruction.

5.15.3. IS machines and media (i.e., diskettes, compact discs, removable hard drives) containing NATO classified information will be stored, marked, handled, and accounted for as other NATO material of the same level according to USSAN 1-69 and this instruction. Do not put actual NATO documents/messages and non-NATO information on the same IS machine or media unless the machine and media is handled as NATO material, the internal files are clearly marked, and everyone having access has been granted access to NATO information. Do not put ATOMAL and non-ATOMAL NATO information on the same IS machine or media unless the machine and media is

handled as ATOMAL, material the internal files are clearly marked, and everyone having access has been granted access to NATO information.

5.16. Technical Surveys. Request electronic counter intelligence technical surveys in accord with AFI 71-101, Volume 3, *Technical Surveillance Countermeasures (TSCM) Program*. *[Reference USSAN 1-69, ATT 1, paragraph 65.3 & 136]*

5.17. Emission Security. Follow the requirements of AFI 33-203, *The Air Force Emission Security Program*. *[Reference USSAN 1-69, ATT1, paragraph 65.4]*

Chapter 6

TRANSMISSION

6.1. General. Handle US documents containing NATO extracts in accordance with DoD 5200.1-R, chapter 7 and AFI 31-401, chapter 6. Transmit CTS, ATOMAL, and NATO Secret documents within the NATO registry system. Apply packaging and mailing restrictions IAW DoD 5200.1-R, chapter 7, and AFI 31-401, chapter 6.

6.2. NATO Confidential. Transmit NATO Confidential information by any means approved for NATO Secret. NATO Confidential can be sent via US Postal Service (USPS) First Class Mail to DoD and US Government organizations within the CONUS. Alaskan, Hawaiian, and APO/FPO addresses are NOT within CONUS. To ensure continuous control by US personnel, transmission outside the CONUS will be through USPS Registered Mail. Geographical addresses and international mail channels will not be used. The same packaging and mailing restriction apply as in the case of US Confidential.

6.3. NATO Restricted. Send NATO Restricted information over secure communication lines. Documents classified NATO Restricted shall be packaged and mailed through USPS First Class Mail and may be single wrapped. To ensure continuous control by US personnel, transmission outside the US will be through USPS First Class Mail through the services' APO/FPO addresses. Geographical addresses and international mail channels will not be used. *[Reference USSAN 1-69, ATT 1, paragraph 97b and 106]*

6.4. Inner Container. Do not enclose US and NATO, or ATOMAL and non-ATOMAL classified in the same inner container.

6.5. Receipts. A receipt is required when sending CTS, ATOMAL, or NATO Secret outside the unit or activity. AF Form 143, 310, or 1565 will satisfy receipt requirements for NATO material. Keep NATO receipt files separate from US receipt files and ATOMAL receipt files separate from non-ATOMAL receipt files. Receipts are not required for NATO Confidential or NATO Restricted unless required by the originator. File receipts in accordance with AFMAN 37-139.

6.6. Handcarrying. Ensure individuals that handcarry NATO classified information are familiar with the procedures and have all appropriate paperwork. Information in USSAN 1-69, ATT 3 to ENCL 2, Section III or DoD 5200.1-R, chapter 7 and AFI 31-401, chapter 6 may be used for briefing and courier certificate requirements. CTS and CTSA material may only be transported across international borders by approved DoD Couriers or diplomatic pouch. Courier letters will be written in English, and if possible, the languages of all other countries the courier will pass through. Installation commanders authorize appropriately cleared couriers to handcarry NATO classified material, to include the use of commercial flights. (This authority may be delegated no lower than unit commanders or staff agency chiefs.) The home unit will maintain a list of all documents being handcarried. *[Reference USSAN 1-69, ATT 1, paragraph 108]*

6.6.1. Military operations. Military commanders may authorize alternate procedures to meet mission requirements in accordance with DoD 5200.1-R, para 1-400; however, mission impact must be demonstrable. In doing so, consideration must be given to risk management factors such as criticality, sensitivity, and value of the information; analysis of the threats both known and anticipated; and vulnerability to exploitation.

6.7. NATO Cryptographic Material. NATO cryptographic material is distributed through COMSEC channels, not through registry channels and remains in the custody of the COMSEC Manager. *[Reference USSAN 1-69, ATT 1, paragraph 109.1]*

Chapter 7

SUBREGISTRIES, CONTROL POINTS, AND COMMUNICATIONS CENTERS

7.1. Subregistry. As an extension of the CUSR, Air Force Subregistries distribute all CTS, ATOMAL, and NATO Secret documents within the activities they service. Designate subregistries either CTSA, CTS, NSA, or NATO Secret.

7.1.1. Installation commanders may delegate appointing authority of subregistries control officer and alternate(s) to the commander or staff agency chief responsible for management of the subregistry. Appoint in writing one subregistry control officer and at least one alternate for each subregistry. *[Reference USSAN 1-69, ATT 1, paragraph 116 & ATT 2, paragraph 27]*

7.1.2. Requests to establish and disestablish AF subregistries must be sent through ISPM channels to HQ USAF/XOFI. A survey report from the local ISPM must be included in the request for establishment. HQ USAF/XOFI forwards the request to the CUSR. *[Reference USSAN 1-69, ATT 1, paragraph 118 & ATT 2, paragraph 30]*

7.1.3. ATOMAL subregistries are authorized to request, receive, and transmit any level of NATO classified. CTS subregistries are authorized to receive CTS and below but not ATOMAL documents. NATO Secret subregistries are authorized to receive NATO Secret and below but not ATOMAL documents.

7.1.4. Subregistries keep a list of names and clearances of control point officers and action officers who routinely receive NATO classified information through them. A duplicate AF Form 2583 may be used. Commanders must notify the subregistry when there is any change in an individual's access. *[Reference USSAN 1-69, ATT 1, paragraph 127(b) & ATT 2, paragraph 31(f)]*

7.1.5. CTS and ATOMAL subregistry control officer may authorize remote or deployed control points to destroy CTS documents. A copy of the destruction certificate and disclosure records will be forwarded to the subregistry immediately after destruction. *[Reference USSAN 1-69, ATT 1, paragraph 113(c)]*

7.2. Control Point. Air Force control points are an extension of their parent subregistry and distribute all CTS , ATOMAL, and NATO Secret documents within the activities they service. A control point designation can not be higher then their parent subregistry. Designate control points either CTSA, CTS, NSA, or NATO Secret.

7.2.1. Commanders will send requests for establishment and disestablishment of control points to the servicing subregistry. A survey report from the local ISPM must be included in the request for establishment. The subregistry commander is the authorization authority. The CUSR must be notified of all ATOMAL control points. *[Reference USSAN 1-69, ATT 1, paragraph 120 & ATT 2, paragraph 32]*

7.2.2. Unit commanders or staff agency chiefs appoint, in writing, one control point officer and at least one alternate for each control point. A copy of the appointment letter will be provided to the servicing subregistry. *[Reference USSAN 1-69, ATT 1, paragraph 116 & ATT 2, paragraph 27]*

7.2.3. Control points keep a list of names and clearances of action officers who routinely receive NATO classified information through them. A duplicate AF Form 2583 may be used. *[Reference USSAN 1-69, ATT 1, paragraph 127(b) & ATT 2, paragraph 31(f)]*

7.3. User. An Air Force NATO user is any office, agency, or individual serviced by a subregistry or control point who requires and is authorized access to NATO classified information to perform assigned missions. Users must protect NATO classified documents in their possession according to the USSAN 1-69 and this instruction.

7.3.1. Subregistries or control points may issue a User CTS and CTSA documents for up to six months. Additional retention shall be justified in writing. *[Reference USSAN 1-69, ATT 1, paragraph 124]*

7.4. Communication Centers.

7.4.1. Brief and grant NATO access to personnel assigned to the level of the material the center handles. Briefings will be accomplished in accordance with paragraphs **4.9.** and **4.10.** of this instruction.

7.4.2. Release CTS and ATOMAL messages to established subregistry or control points for accountability purposes. NS messages may be released directly to addressees with notification to the subregistry. Notification to the subregistry may be made monthly with a copy of the communication center's message log. NATO Confidential/Restricted may go directly to the addressee, no subregistry notification required.

7.4.3. Record copies of non-ATOMAL NATO classified messages may be maintained with other non-record US classified messages according to the communications center's controlling directive.

7.4.4. Communication centers supporting ATOMAL subregistries and control points must maintain, and implement Allied Communications Publication (ACP) 122 NATO Supplement 2A, *Handling of ATOMAL Information with Classified Communication Centers,* and establish written procedures for handling of ATOMAL messages within the communication center.

7.4.4.1. Maintain record copies of ATOMAL messages separate from all other US and NATO messages. Record the destruction of these messages, as appropriate, according to ACP 122, NATO Supplement 2A.

7.4.4.2. Maintain a separate ATOMAL log listing all ATOMAL documents.

Chapter 8

SECURITY INCIDENTS

8.1. Reporting. Anyone discovering a security violation involving NATO classified information must immediately report it to their supervisor, security manager, or commander. The incident must be reported to the servicing ISPM by the end of the first duty day. *[Reference USSAN 1-69, ATT 1, paragraph 150]*

8.1.1. When there is a compromise or loss of NATO classified information, immediately notify HQ USAF/XOFI through ISPM channels. HQ USAF/XOFI will notify the CUSR. *[Reference USSAN 1-69, ATT 1, paragraph 151]*

8.1.1.1. Before a security investigation report of a compromise or loss is closed, the report must be sent through ISPM channels to HQ USAF/XOFI for review within 40 calendar days from the date of notification. If the investigative report will not reach HQ USAF/XOFI within 40 days, provide a written status report with an estimated completion date. HQ USAF/XOFI will forward a copy of completed reports to the CUSR. *[Reference USSAN 1-69, ATT 1, paragraph 156b, 156c, & ATT 2, paragraph 61]*

8.1.2. Immediately notify the supporting AFOSI activity when there are any indications or suspicions of espionage or criminal activity. *[Reference USSAN 1-69, ATT 1, paragraph 154(b)]*

8.2. Investigations. Conduct investigations of security incidents involving NATO information in accordance with DoD 5200.1-R, chapter 10 and AFI 31-401, chapter 9. *[Reference USSAN 1-69, ATT 1, paragraph 150]*

8.2.1. Investigations must be directed by the commander of the organization in which the incident occurred. If the commander is involved, his or her supervisor will initiate the investigation.

8.2.2. The ISPM, and the unit will maintain a copy of security incident reports involving NATO information. If the incident involves CTS, ATOMAL, or NATO Secret information provide a copy of the report to the servicing subregistry. Retain security incident reports in accordance with AFMAN 37-139. *[Reference USSAN 1-69, ATT 1, paragraph 152]*

8.3. NATO Restricted. MAJCOM ISPMs establish procedures for reporting, processing, and closing incidents involving NATO Restricted. Incidents involving espionage and deliberate compromise will be reported IAW para 8.1 of this instruction.

8.4. Cryptographic Material. See AFI 33-212, *Reporting COMSEC Deviations.*

MARVIN R. ESMOND, Lt Gen, USAF
DCS/Air & Space Operations

Attachment 1

GLOSSARY OF REFERENCE AND SUPPORTING INFORMATION

References

AC/35-D/1004, *NATO Security Directive*

ACP 122 NATO Supplement 2A, *Handling of ATOMAL Information with Classified Communication Centers*

DoDD 5100.55, *United States Security Authority for North Atlantic Treaty Organization Affairs*

DoD 5200.1-R, *Information Security Program*

DoD 5220.22-M, *National Industrial Security Operating Manual (NISPOM)*

USSAN 1-69, *United States Implementation of NATO Security Procedures*

AFI 16-201, *Foreign Disclosure of Classified and Unclassified Military Information to Foreign Governments and International Organizations*

AFPD 31-4, *Information Security Program*

AFI 31-401, *Managing the Information Security Program*

AFI 31-501, *Personnel Security Program Management*

AFI 33-202, *Computer Security*

AFI 33-203, *The Air Force Emission Security Program*

AFI 33-212, *Reporting COMSEC Deviations*

AFI 61-205, *Sponsoring or Cosponsoring, Conducting and Presenting DoD Related Scientific and Technical Papers at Unclassified and Classified Conferences, Symposia, and Other Similar Meetings*

AFI 71-101, Volume 3, *Technical Surveillance Countermeasures (TSCM) Program*

AFMAN 37-139, *Records Disposition Schedule*

Abbreviations and Acronyms

ACP—Allied Communications Publication

AF—Air Force

AFI—Air Force Instruction

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AFR—Air Force Regulation

ANACI—Access National Agency Check with Written Inquiries and Credit Check

API—Advance Planning Information

CONUS—Continental United States

CTSA—COSMIC Top Secret ATOMAL

CTS—COSMIC Top Secret

CUSR—Central United States Registry

DRU—Direct Reporting Units

FOA—Field Operating Agencies

FRD—Formerly Restricted Data

HQ USAF/XOFI—Headquarters Air Force, Chief, Information Security Division

HQ USAFE/SFI—Headquarters United States Air Forces in Europe, Directorate of Security Forces, Security Programs Division

IS—Information Systems

ISPM—Information Security Program Manager

LAA—Limited Access Authorization

MAJCOM—Major Command

NAC—National Agency Check

NACIC—National Agency Check with Written Inquiries and Credit Checks

NACLC—National Agency Check, Local Agency Checks and Credit Check

NATO—North Atlantic Treaty Organization

NCA—NATO Confidential ATOMAL

NISPOM—National Industrial Security Operating Manual

NPLO—NATO Production and Logistics Organization

NR—NATO Restricted

NS—NATO Secret

NSA—NATO Secret ATOMAL

OCA—Original Classification Authority

PCS—Permanent Change of Station

SAF/AA—Administrative Assistant to the Secretary of the Air Force

SAF/IA—Deputy Under Secretary of the Air Force, International Affairs

SCIF—Sensitive Compartmented Information Facilities

SIF—Security Information File

SF—Standard Form

SSBI—Single Scope Background Investigation

TDY—Temporary Duty

TSCM—Technical Surveillance Countermeasures

U—Unclassified

USPS—United States Postal Service

USSAN—United States Security Authority for NATO Affairs

Attachment 2

SAMPLE NATO SECURITY CLEARANCE CERTIFICATION CERTIFICATE

(Official Letter Head)

MEMORANDUM FOR

FROM:

SUBJECT: NATO Security Clearance Certificate

1. Full Name:

Date and Place of Birth:

Has been granted a security clearance by the Government of the United States of America, in accordance with current NATO regulations, including the Security Annex to C-M(64)39, in the case of ATOMAL information, and is therefore declared suitable to be entrusted with information classified up to and including (level of classification).

2. The validity of this certificate will expire not later than (no more than five years from the date of the individual's inspection).

(signature block of a NATO access granting authority)

NOTE: classification will be:

a. COSMIC Top Secret

b. COSMIC Top Secret ATOMAL

c. NATO Secret

d. NATO Secret ATOMAL

e. NATO Confidential

f. NATO Confidential ATOMAL

Attachment 3

SAMPLE AF FORM 2583

REQUEST FOR PERSONNEL SECURITY ACTION

AUTHORITY: 10 U.S.C. 8012; 44 U.S.C. 3101; and EO 9397.
PRINCIPAL PURPOSES: To identify investigation, security clearance, unescorted entry requirements, and special access program authorizations.
ROUTINE USES: To request personnel security investigations, record emergency or limited access authorization, entry to restricted areas, and to record special access program authorizations. SSN is used for positive identification of the individual and records.
DISCLOSURE IS VOLUNTARY: Failure to information and SSN could result in assignment to less sensitive duties.

I. IDENTIFYING INFORMATION

1. NAME (Last, First, Middle, Maiden)	2. ORGANIZATION OR FIRM SPONSOR
MacGillivray, Doar E.	HQ USAFE/SF

3. GRADE	4. SSN	5. CITIZENSHIP				
TSgt	999-99-9999	X	US CITIZEN		IMMIGRANT ALIEN	NON-US NATIONAL

6. DATE OF BIRTH	7. PLACE OF BIRTH (City, State, and Country)
27 Nov 68	Phelps, NY

II. INVESTIGATION, CLEARANCE, ELIGIBILITY, ENTRY AND ACCESS REQUIREMENTS

8. INVESTIGATION REQUIREMENT		9. CLEARANCE, ENTRY OR ACCESS REQUIREMENT			
	NATIONAL AGENCY CHECK (NAC)		ONE-TIME ACCESS		LIMITED ACCESS
	NATIONAL AGENCY CHECK-WRITTEN INQUIRIES (NACI)		INTERIM CLEARANCE		SPECIAL ACCESS
	BACKGROUND INVESTIGATION (BI)	X	FINAL CLEARANCE		UNESCORTED ENTRY
X	SPECIAL BACKGROUND INVESTIGATION (SBI)		TOP SECRET		PRORITY A
	BI PERIODIC REINVESTIGATION (PR)		SECRET		PRORITY B
	SBI PERIODIC REINVESTIGATION (PR)		CONFIDENTIAL		PRORITY C

III. LCCAL FILES CHECK

10. TO:	11. FROM:

12. DATE	13. TYPED NAME, GRADE AND TITLE OF REQUESTER	14. SIGNATURE
1 Feb 99	Helen Adams, SMSgt, USAF HQ USAFE/SF Security Manager	

IV. MEDICAL RECORDS CHECK

15. I CERTIFY a medical records check required by DOD 5200.2R/AFR 205-32, has been completed and no information exists, unless shown in Section VII, which would preclude the granting of a security clearance, unescorted entry to restricted areas, or access to special program classified information.

16. DATE	17. TYPED NAME AND GRADE OF BASE DIRECTOR, MEDICAL SERVICES	18. SIGNATURE

V. SECURITY POLICE RECORDS CHECK

19. I CERTIFY a security police records check required by AFR 205-32, has been completed and no information exists, unless shown in Section VII, which would preclude the granting of a security clearance, unescorted entry to restricted areas, or access to special program classified information.

20. DATE	21. TYPED NAME AND GRADE OF SECURITY POLICE OFFICAL	22. SIGNATURE

VI. ACCESS AUTHORIZATION

	ONE-TIME ACCESS		LIMITED ACCESS		CNWDI	X	NATO		SIOP-ESI	
							CTSA		CONTINUING	ONE-TIME

23. I CERTIFY the named individual requires access to the above special program(s), meets all investigative and clearance requirements, and has been briefed on program responsibilities as outlined in the governing directive. If applicable, emergency or limited access is necessary and will not endanger the national security.

24. DATE	25. TYPED NAME, GRADE AND TITLE OF APPROVING AUTHORITY	26. SIGNATURE

27. DATE	28. TYPED NAME, GRADE AND TITLE OF SPECIAL ACCESS PROGRAM CERTIFYING OFFICIAL	29. SIGNATURE
1 Feb 99	Richard S. Rathbun, Col, USAF Director of Security Forces	

VII. REMARKS

30. *(If more space is needed, use reverse and show item number being continued)*

Briefed according to USSAN 1-69 on 1 Feb 99.

ATOMAL rebriefed on 31 Jan 2000.

AF Form 2583, MAR 87 *(EF)* PREVIOUS EDITION WILL BE USED.

Attachment 4

SAMPLE INITIAL NATO SECURITY BRIEFING

1. NATO Defined:

a. On April 4, 1949, the North Atlantic Treaty was signed and the North Atlantic Treaty Organization (NATO) was formed. The North Atlantic Treaty is the framework for wide cooperation among its members. NATO is more than a military alliance formed to prevent aggression, or to repel aggression forces should the need arise. It also provides for continuing joint action in the political, economic, and social fields.

b. The total membership of NATO includes: Belgium, Canada, Czech Republic, Denmark, France, Germany, Greece, Hungary, Iceland, Italy, Luxembourg, Netherlands, Norway, Poland, Portugal, Spain, Turkey, United Kingdom, and the United States.

2. Air Force Instruction and Implementing United States Security Authority for NATO Affairs Instruction: The following publications contain requirements for safeguarding and handling NATO classified material. Consult these directives for detailed procedures on safeguarding and handling NATO classified material.

a. USSAN Instruction 1-69, Safeguarding NATO Classified Information.

b. AFI 31-406, Applying NATO Protection Standards.

3. USSAN Instruction 1-69: The USSAN Instruction 1-69 is the basic NATO security procedures for protecting NATO classified information. The left column contains NATO protection and handling requirements while the right column contains the DoD clarification or implementing instructions. Neither the left or right columns should be used separately without reference to the corresponding column.

4. AFI 31-406: Air Force Instruction 31-406 contains Air Force unique guidance needed to supplement USSAN 1-69 and DoD Directive 5100.55. All these references together describe how to protect and handle NATO classified information and information releasable to NATO organizations.

5. Granting Access to NATO Classified:

a. Access to NATO classified information must be limited to a need-to-know and minimum number of individuals.

b. Individuals granted NATO access must have a US security clearance equal to the level of NATO classified information to which access is being granted.

c. Access granting authorities record access authorization on AF Form 2583.

6. Dissemination of Material: NATO material can be disclosed only to personnel authorized such access. Holders of NATO material are responsible for determining if individuals requiring access have been properly cleared.

7. Types and Classification of NATO Information:

a. NATO Marking. The word NATO is a marking that signifies the information:

(1) Is the property of NATO and may not be passed outside of the NATO organization except by the originator or with the originator's consent.

(2) Is subject to the security protection set forth in NATO security regulations.

(3) Normally, only the last US organization having custody of the document is authorized to apply the NATO markings before it is released to a NATO organization.

b. Classification of NATO Information. NATO information is classified COSMIC Top Secret (CTS), NATO Secret (NS), NATO Confidential (NC), and NATO Restricted (NR). The definitions of the first three classification levels are similar to those of US classifications. NR is a security classification applied by only NATO to information and material that requires a degree of protection, similar to that for "For Official Use Only."

c. ATOMAL. ATOMAL is a term used to designate "Restricted Data" or "Formerly Restricted Data" provided by the US and the United Kingdom to NATO Components. ATOMAL information is classified COSMIC Top Secret ATOMAL (CTSA), NATO Secret ATOMAL (NSA), or NATO Confidential ATOMAL (NCA).

8. Breaches of Security. It is very important that any breach of security that may come to an individual's attention is at once reported to a supervisor or security manager and all classified information gets immediately controlled.

9. Procedural Requirements. Requirements already specified for US classified information apply to NATO material. There are additional requirements for NATO to ensure that people do not gain unauthorized access to it.

10. Extracts. Mark in the same manner required for other NATO classified extracts. Identify the source NATO document the extract was taken from on the "Derived From" line and include any declassification/downgrading instruction.

11. Reproduction. Limit reproduction of NS, NSA, NC, and NCA documents only to quantities sufficient to meet current mission requirements, when there are no reproduction limitations imposed. Do not reproduce CTS or CTSA documents.

12. Control. Designated NATO subregistries and control points receive, record, handle, and distribute NS and above information.

13. Accountability. COSMIC subregistries and control points keep records of origination, receipt, transmission, change of classification or declassification, and destruction of all CTS documents.

14. Excerpts of US Code. Excerpts from the following US Codes apply to NATO material:

a. Title 18 U.S.C. Section 793, Gathering, Transmitting, or Losing Defense Information.

b. Title 18 U.S.C. Section 794, Gathering or Delivering Defense Information to Aid Foreign Governments.

c. Title 50 U.S.C. Section 783 Offenses.

Attachment 5

SAMPLE ATOMAL BRIEFING

Use to conduct initial and annual rebriefing for personnel who have ATOMAL access, regardless of the level. Record this annual briefing on AF Form 2583, block 30.

1. **ATOMAL Information.** The words “Atomic Information” refer to information designated by the US Government as “Restricted Data” or “Formerly Restricted Data” in accordance with the Atomic Energy Act of 1954. The word “ATOMAL” refers to atomic information communicated by the Governments of the United States and the United Kingdom to NATO under the Agreement Between the Parties to the North Atlantic Treaty for Co-Operation Regarding Atomic Information.

2. **Classification.** ATOMAL information may be classified as COSMIC Top Secret ATOMAL (CTSA), NATO Secret ATOMAL (NSA), or NATO Confidential ATOMAL (NCA).

3. **Markings.** Place the “ATOMAL” after the appropriate NATO classification designation at the top and bottom of each page containing ATOMAL information. The last custodian before transmission to NATO is responsible for the ATOMAL marking.

4. **Extracts.** Mark in the same manner required for other NATO classified extracts. Identify the source NATO document the extract was taken from on the “Derived From” line and write the Restricted Data or Formerly Restricted Data warning notice (see DoD 5200.1-R, paragraph 5-208) and the statement "This Document Contains (classification) ATOMAL Information."

5. **Reproduction.** Limit reproduction of NSA and NCA documents only to quantities sufficient to meet current mission requirements, when there are no reproduction limitations imposed. Do not reproduce CTSA documents.

6. **Disclosure.** Before disclosing ATOMAL information, ensure the person has a need-to-know the information, and is properly cleared for the level of material involved. Ensure a disclosure record is attached to each accountable ATOMAL document. Use AF Form 144; remove it from the document before transfer or destruction.

7. **Packaging.** Use the same receipt form required for other NATO classified documents. Prepare for transmission using the “double opaque” concept.

8. **Control.** Designated ATOMAL subregistries and control points receive, record, handle, and distribute ATOMAL documents.

9. **Accountability.** ATOMAL subregistries and control points keep records of origination, receipt, transmission, change of classification or declassification, and destruction of all ATOMAL documents.

10. **Excerpts From the Atomic Energy Act of 1954.**

a. Title 42 U.S.C. Section 2274, Communication of Restricted Data.

b. Title 42 U.S.C. Section 2275, Receipt of Restricted Data.

c. Title 42 U.S.C. Section 2276, Tampering With Restricted Data

d. Title 42 U.S.C. Section 2277, Disclosure of Restricted Data.

Attachment 6

SAMPLE NATO ACCESS DEBRIEFING

1. Now that your access to _____ is being terminated, you must return all NATO classified documents you have in your possession. Return these documents to _____.

2. Your responsibility does not end with the turn-in of NATO classified materials. You no longer have a reason or authority to discuss NATO classified information with anyone, to include persons you know to be properly cleared. Do not discuss your past work.

3. You are required by law to immediately report any attempt by an unauthorized individual to solicit NATO information from you. Report such an attempt to the nearest Air Force Office of Special Investigations (AFOSI). If you are being separated from military or civil service, report attempts to the nearest office of the Federal Bureau of Investigations (FBI).

4. If you prepare material for public release that may or might contain NATO classified information, you should submit the material for a security review of the nearest Air Force Public Affairs Office or the Secretary of the Air Force, Public Affairs Secretary.

5. (For ATOMAL) You have had access to information relating to the national defense (including Restricted Data) which is protected by statute. These statutes make it a crime to unlawfully communicate information of national defense to any person when there is reason to believe that the information will be used to the injury of the United States or to the advantage of a foreign government. The penalties prescribed for violations of these statutes, through willful acts or gross negligence, vary according to the statute, the circumstances, and the information involved.

6. In a few moments you will sign AF Form 2587 officially terminating your NATO access. You will acknowledge that any unauthorized disclosure of NATO classified information is prohibited and punishable by law.